

The Information Commissioner's response to the Department for Work and Pensions consultation on 'Pension dashboards: working together for the consumer'

Overview

1. The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 2018 ("DPA"), the Freedom of Information Act 2000 ("FOIA"), the Environmental Information Regulations ("EIR") and the Privacy and Electronic Communications Regulations 2003 ("PECR"). She is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.
2. The Information Commissioner welcomes the opportunity to respond to Department for Work and Pensions' consultation on 'Pensions Dashboards: working together for the consumer'. She recognises there is a public interest in recipients of private pension schemes having better access to their pension information and having a more transparent understanding of their financial future. Access to personal data is a key principle of data protection and the Commissioner welcomes the Government's initiative to facilitate and improve people's access to accurate and useful information about their pensions. She also appreciates the opportunity to reinforce data protection principles in the financial industry related to private pensions. This response focuses on those areas that raise data protection considerations.

Comment

3. It is essential that the proposed dashboards operate in compliance with data protection law to respect individuals' rights to privacy and personal data protection. We are pleased that the consultation raises the importance of adherence to the rights of the individual and principles set out in the Data Protection Act 2018 and GDPR. We welcome that prominence is given to these considerations which should be integral to the design and governance of the dashboards.

We provide relevant [guidance on data protection by design and default](#).

4. The consultation states the dashboards will not store any data and be used “for presentational purposes only.” There is an overview of the ‘dashboard ecosystem’ where it is envisaged that the Pension Finder Service (PFS) will act like a search engine and the details of the values of a pension will not pass through it. Paragraph 141 refers to the pension schemes as the controller. We note this consultation process is an opportunity for the parties involved in the dashboards to have clearly defined roles, whether controllers or processors. There could be a risk of ambiguity as to whether the Department, Single Financial Guidance Body or proposed industry delivery group is leading on governance. It is important there is no ambiguity within the dashboard ecosystem with multiple parties involved. There should be no fragmentation where some parties acknowledge they are processing personal data and others believe they are not. We provide detailed [guidance on controllers and processors](#) and [guidance on what is personal data](#). We also provide [guidance on accountability and governance](#).
5. We note the consultation is clear that the Department ultimately expects to include ‘Check Your State Pension’ data as part of the service.
6. Our [Code of Practice on data sharing](#) may be relevant to this proposal. We are currently updating the code to bring it in line with the requirements of the GDPR and as such it should be used with caution. The updated code, which is due for consultation in early 2019, will explain and advise on changes to data protection legislation, where these changes are relevant to data sharing, and will also provide practical guidance in relation to data sharing and promote good practice.
7. As this dashboard project has the aim of expanding beyond private pensions to incorporate State Pension data, the Department may consider in their Personal Information Charter or by any other appropriate means if future customers have sufficient notice and understanding of how their data is being used or may be used in future.
8. We are pleased the consultation makes specific reference to individual’s right to data portability and “principles of accuracy, storage, access and security”. We provide [guidance on the rights of individuals](#). In the design of the dashboards, we would urge attention be given to accountability. Some people interpret GDPR Article 5(2) on accountability as a data protection principle itself and we think it

would be helpful to bear that principle in mind particularly when documenting agreements between the various parties of the dashboard ecosystem.

9. The consultation discusses consent and that access to data should only be granted if the data subject gives specific consent. Where the consultation references it becoming mandatory for certain pension schemes to become part of the dashboards, it is important this is not confused with it being mandatory for data subjects to consent to accessing the dashboards. We have produced detailed [guidance on consent](#). The Department may also consider if other lawful bases for processing are relevant at various points within the dashboard ecosystem.
10. Data Privacy Impact Assessments (DPIAs) form part of the 'data protection by default and by design' and accountability approach under GDPR. Article 35 requires organisations to carry out a DPIA before carrying out types of processing likely to result in a high risk to the rights and freedoms of individuals in specified circumstances. It will be for the Department to decide whether the threshold of requiring a DPIA is reached but factors to consider would be the use of this new dashboard's design and incorporation of vast amounts of financial personal data. Detailed [guidance about DPIAs](#) is available on our website.
11. In circumstances where personal data is processed it must be compliant with data protection legislation. We recommend the Department ensures that parties in the dashboard ecosystem have clearly defined roles and understanding of their responsibilities under data protection legislation. We recommend the Department considers carrying out a DPIA. We recommend careful consideration is given to security and accuracy of personal data; and data protection by design and default is an overriding principle of the dashboard design.

January 2019